

Welcome to the PIA for FY 2011!

Congress passed the E-Government Act of 2002 to encourage the use of Web-based Internet applications or other information technology by Government agencies, with the intention of enhancing access to government information and services and increasing the effectiveness, efficiency, and quality of government operations.

To combat public concerns regarding the disclosure of private information, the E-Government Act mandated various measures, including the requirement that Federal agencies conduct a Privacy Impact Assessment (PIA) for projects with information technology systems that collect, maintain, and/or disseminate "personally identifiable information" of the public. Personally identifiable information, or "personal information," is information that may be used to identify a specific person.

The Privacy Act and VA policy require that personally identifiable information only be used for the purpose(s) for which it was collected, unless consent (opt-in) is granted. Individuals must be provided an opportunity to provide consent for any secondary use of information, such as use of collected information for marketing.

Directions:

VA 6508 is the directive which outlines the PIA requirement for every System/Application/Program.

If you find that you can't click on checkboxes, make sure that you are: 1) Not in "design mode" and 2) you have enabled macros.

PIA Website: http://vawww.privacy.va.gov/Privacy_Impact_Assessments.asp

Roles and Responsibilities:

Roles and responsibilities for the specific process are clearly defined for all levels of staff in the VA Directive 6508 referenced in the procedure section of this document.

- a. The Privacy Officer is responsible for the overall coordination and review of the PIA to ensure compliance with VA Directive 6508.
- b. Records Officer is responsible for supplying records retention and deletion schedules.
- c. Information Technology (IT) staff responsible for the privacy of the system data will perform a PIA in accordance with VA Directive 6508 and to immediately report all anomalies to the Privacy Service and appropriate management chain.
- d. Information Security Officer (ISO) is responsible for assisting the Privacy Officer and providing information regarding security controls.
- e. The CIO is responsible for ensuring that the systems under his or her jurisdiction undergo a PIA. This responsibility includes identifying the IT systems; coordinating with the Privacy Officer, Information Security Officer, and others who have concerns about privacy and security issues; and reviewing and approving the PIA before submission to the Privacy Service.

Definition of PII (Personally Identifiable Information)

Information in identifiable form that is collected and stored in the system that either directly identifies and individual by name, address, social security number, telephone number, e-mail address, biometric identifiers, photograph, or other unique numbers, codes or characteristics or combined, indirect identify an individual such as a combination of gender, race, birth date, geographical indicators, license number is also considered PII.

Macros Must Be Enabled on This Form

Microsoft Office 2003: To enable macros, go to: 1) Tools > Macros > Security - Set to Medium; 2) Click OK; 3) Close the file and when reopening click on Enable Macros at the prompt.

Microsoft Office 2007: To enable macros, go to: 1) Office Button > Prepare > Excel Options > Trust Center > Trust Center Settings > Macro Settings > Enable

All Macros; 2) Click OK

Final Signatures

Final Signatures are digitally signed or wet signatures on a case by case basis. All signatures should be done when all modifications have been approved by the VA Privacy Service and the reviewer has indicated that the signature is all that is necessary to obtain approval.

Privacy Impact Assessment Uploaded into SMART

Privacy Impact Assessments should be uploaded into C&A section of SMART.

All PIA Validation Letters should be emailed to christina.pettit@va.gov to received full credit for submission.

(FY 2011) PIA: System Identification

Program or System Name: CDCO > AITC > VA > Defense Finance Accountability Service (DFAS) Secure ePayroll Transmission
OMB Unique System / Application / Program Identifier (AKA: UPID #): 029-00-01-19-01-1330-00

Description of System/ Application/ Program: The purpose of the VA's Defense Finance Accountability Service (DFAS) Secure ePayroll Transmission application is to provide a solution that consists of the necessary software and scanners to allow VA payroll documents to be sent in a secure manner to Defense Civilian Pay System (DCPS). The solution shall support 202 payroll offices throughout the VA, and shall include hardware (scanners), software, dedicated support services, training, and standard maintenance for both the hardware and software.

Facility Name: Austin Information Technology Center (AITC) CDCO

Title:	Name:	Phone:	Email:
Privacy Officer:	Amy Howe	512-326-6217	amy.howe1@va.gov
Information Security Officer:	Neil Cruz	(202) 461-6254	neil.cruz@va.gov
System Owner/ Chief Information Officer:	John Rucker	512-326-6422	John.Rucker@va.gov
Data Owner:	Roy Coles	202-461-6105	roy.coles@va.gov
Other Titles:			

Person Completing Document:

Other Titles: Program Manager

Date of Last PIA Approved by VACO Privacy Services: (MM/YYYY)

n/a - first PIA for DFAS

Date Approval To Operate Expires:

n/a (not yet determined - new system)

What specific legal authorities authorize this program or system:

Statutory provisions, Executive Order 12191 (45 FR 7997 (Feb. 6, 1980)) and other Executive Orders of the President, and rules and regulations of certain Federal regulatory departments and agencies.

What is the expected number of individuals that will have their PII stored in this system:

300000+ VA Employees
Operations/Maintenance

Identify what stage the System / Application / Program is at:

The approximate date (MM/YYYY) the system will be operational (if in the Design or Development stage), or the approximate number of years the system/application/program has been in operation.

04/2011

Is there an authorized change control process which documents any changes to existing applications or systems?

Yes

If No, please explain:

Has a PIA been completed within the last three years?

N/A: First PIA

Date of Report (MM/YYYY):

02/2011

Please check the appropriate boxes and continue to the next TAB and complete the remaining questions on this form.

- ☐ Have any changes been made to the system since the last PIA?
- ☐ Is this a PIV system/application/program collecting PII data from Federal employees, contractors, or others performing work for the VA?
- ☒ Will this system/application/program retrieve information on the basis of name, unique identifier, symbol, or other PII data?
- ☒ Does this system/application/program collect, store or disseminate PII/PHI data?
- ☒ Does this system/application/program collect, store or disseminate the SSN?

If there is no Personally Identifiable Information on your system, please complete TAB 7 & TAB 12. (See Comment for Definition of PII)

(FY 2011) PIA: System of Records

Is the data maintained under one or more approved System(s) of Records? If the answer above no, please skip to row 15.

Yes

For each applicable System(s) of Records, list:

1. All System of Record Identifier(s) (number):

27VA047

2. Name of the System of Records:

Personnel and Accounting Pay System-VA

3. Location where the specific applicable System of Records Notice may be accessed (include the URL):

http://www.rms.oit.va.gov/SOR_Records/27VA047.asp

Have you read, and will the application, system, or program comply with, all data management practices in the System of Records Notice(s)?

Yes

Does the System of Records Notice require modification or updating?

No

(Please Select Yes/No)

Is PII collected by paper methods?

Yes

Is PII collected by verbal methods?

Yes

Is PII collected by automated methods?

Yes

Is a Privacy notice provided?

Yes

Proximity and Timing: Is the privacy notice provided at the time of data collection?

Yes

Purpose: Does the privacy notice describe the principal purpose(s) for which the information will be used?

Yes

Authority: Does the privacy notice specify the effects of providing information on a voluntary basis?

Yes

Disclosures: Does the privacy notice specify routine use(s) that may be made of the information?

Yes

(FY 2011) PIA: Notice

Please fill in each column for the data types selected.

Data Type	Collection Method	What will the subjects be told about the information collection?	How is this message conveyed to them?	How is a privacy notice provided?
Veteran or Primary Subject's Personal Contact Information (name, address, telephone, etc)	Electronic/File Transfer	Provided for hire (benefits info)	Written	Written
Family Relation (spouse, children, parents, grandparents, etc)	Paper	Provided for job application or for hire	Written	Written
Service Information	Paper	Provided for hire (benefits info)	Written	Written
Medical Information	N/A			
Criminal Record Information	N/A			
Guardian Information	N/A			
Education Information	Paper	Provided for hire	Written	Written
Benefit Information	Paper	Provided for hire (benefits info)	Written	Written
Other (Explain)				

Data Type	Is Data Type Stored on your system?	Source (If requested, identify the specific file, entity and/or name of agency)	Is data collection Mandatory or Voluntary?	Additional Comments
Veteran or Primary Subject's Personal Contact Information (name, address, telephone, etc)	Yes	VA Files / Databases (Identify file)	Mandatory	PAID, OLDE, FUM
Family Relation (spouse, children, parents, grandparents, etc)	Yes	VA Files / Databases (Identify file)	Mandatory	PAID, OLDE, FUM
Service Information	Yes	VA Files / Databases (Identify file)	Mandatory	PAID, OLDE, FUM
Medical Information	No			

Criminal Record Information	No			
Guardian Information	No			
Education Information	Yes	VA Files / Databases (Identify file)	Mandatory	PAID, OLDE, FUM
Benefit Information	Yes	VA Files / Databases (Identify file)	Mandatory	PAID, OLDE, FUM
Other (Explain)				
Other (Explain)				
Other (Explain)				

(FY 2011) PIA: Data Sharing

Organization	Name of Agency/Organization	Do they access this system?	Identify the type of Data Sharing and its purpose.	Is PII or PHI Shared?	What is the procedure you reference for the release of information?
Internal Sharing: VA Organization	DCPS	No	File Transfer	PII	Info passed is internal to VA and needed to process employee payroll
Other Veteran Organization	NA				
Other Federal Government Agency	NA				
State Government Agency	NA				
Local Government Agency	NA				
Research Entity	NA				
Other Project / System					
Other Project / System					
Other Project / System					

(FY 2011) PIA: Access to Records

Does the system gather information from another system?	Yes
Please enter the name of the system:	Electronic /File transfer from 202 VA Payroll Sites
Per responses in Tab 4, does the system gather information from an individual?	Yes
If information is gathered from an individual, is the information provided:	<input checked="" type="checkbox"/> Through a Written Request <input checked="" type="checkbox"/> Submitted in Person <input checked="" type="checkbox"/> Online via Electronic Form
Is there a contingency plan in place to process information when the system is down?	No

(FY 2011) PIA: Secondary Use

Will PII data be included with any secondary use request?

No

☐ Drug/Alcohol Counseling ☐ Mental Health ☐ HIV

if yes, please check all that apply:

☐ Research ☐ Sickle Cell ☐ Other (Please Explain)

Describe process for authorizing access to this data.

Answer:

(FY 2011) PIA: Program Level Questions

Does this PIA form contain any sensitive information that could cause harm to the Department of Veterans Affairs or

No

If Yes, Please Specify:

Explain how collected data are limited to required elements:

Answer: Data elements are limited to active employees of the VA and input by valid VA representatives.

How is data checked for completeness?

Answer: Employee review and data dedits within EEX and OLDE input subsystems check the data for completeness and logic checks before being passed to the Edit and update subsystem.

What steps or procedures are taken to ensure the data remains current and not out of date?

Answer: EEX and OLDE input transactions update PAID daily. All employees have access to their service record information, and they may utilize EEX or contact their HR/Payroll agents to updated information.

How is new data verified for relevance, authenticity and accuracy?

Answer: Data edits are placed within the EEX and OLDE input subsystems that check the entered data for relevance, authenticity and accuracy before being passed to the Edit and Update subsystem. In the Edit and Update subsystem, the data is again edited and checked for relevance and authenticity before being added to the PAID records.

Additional Information: (Provide any necessary clarifying information or additional explanation for this section.)

Answer:

(FY 2011) PIA: Retention & Disposal

What is the data retention period?

Answer: PAID data is retained on line for all active VA employees at the Austin Information Technology Center. After one Pay Period for a VA employee who is no longer an active employee and 26 Pay Periods for a DFAS employee, the data is archived on tape, transferred to a records facility for two more years, and disposed of in accordance with disposition authorization approved by the Archivist of the United States.

Explain why the information is needed for the indicated retention period?

Answer: The PAID data is used to process payroll data; sometimes corrections for past actions need to be accomplished.

What are the procedures for eliminating data at the end of the retention period?

Answer: Paper documents may be shredded or burned and record destruction is documented in accordance with NARA guidelines. Selected destruction methods for other data media comply with NCSC-TG-025 Version-2/VA Policy. If a degausser is not available, the media is destroyed by smelting, pulverization or disintegration. Other IT equipment and electronic storage media are sanitized in accordance with procedures of the NSA/Central Security Service Media Declassification~ and Destruction Manual and certified that the data has been removed or that it is unreadable. Certification identifies the Federal Information Processing (FIP) item cleared. FIP equipment is not excessed, transferred, discontinued from rental or lease, exchanged, or sold without certification.

Where are these procedures documented?

Answer: The disposition authority is documented in Record Control Schedule 10-1, Section XLIII-1 and XLIII-2. Disposition instructions and procedures for electronic media are documented in NCSC-TG-025 Version-2/VA Policy, VA Form 0751, Information Technology Equipment Sanitization Certificate.

How are data retention procedures enforced?

Answer: No records are disposed/destroyed without the approval of the facility's Record Control Manager. All records are disposed of in accordance with VA Policy and disposition authority (RCS 10-1). Archived and retired records are maintained in accordance with VA Policy.

Has the retention schedule been approved by the National Archives and Records Administration (NARA)

Yes

Additional Information: (Provide any necessary clarifying information or additional explanation for this section.)

Answer:

(FY 2011) PIA: Children's Online Privacy Protection Act (COPPA)

Will information be collected through the internet from children under age 13?

No

If Yes, How will parental or guardian approval be obtained?

Answer:

(FY 2011) PIA: Security

Is the system/application/program following IT security Requirements and procedures required by federal law and policy to ensure that information is appropriately secured. Yes

Has the system/application/program conducted a risk assessment, identified appropriate security controls to protect against that risk, and implemented those controls.. Yes

Is security monitoring conducted on at least a quarterly basis to ensure that controls continue to work properly, safeguarding the information? Yes

Is security testing conducted on at least a quarterly basis to ensure that controls continue to work properly, safeguarding the information? Yes

Are performance evaluations conducted on at least a quarterly basis to ensure that controls continue to work properly, safeguarding the information? Yes

If 'No' to any of the 3 questions above, please describe why:

Answer:

Is adequate physical security in place to protect against unauthorized access? Yes

If 'No' please describe why:

Answer:

Explain how the project meets IT security requirements and procedures required by federal law.

Answer: The DFAS system is housed at the AITC and is a part of the PAID system. At the project level, security is provided by the Austin Information Technology Center (AITC). DFAS operates within the AITC LAN environment, and will be granted a full Authority to Operate upon completion of testing and adocument review. DFAS is included in AITC password management and user authentication processes. Access is granted to individuals with AITC TSO access and written authorization from their supervisor. Facility staff determines level of access for individuals to view and report on their data. In addition, in accordance with the contract between the contractor and the government, all contractors with access to DFAS information are required to meet the AITC contractor security requirements.

Explain what security risks were identified in the security assessment? (Check all that apply)

- | | | |
|---|---|--|
| <input type="checkbox"/> Air Conditioning Failure | <input checked="" type="checkbox"/> Data Disclosure | <input type="checkbox"/> Hardware Failure |
| <input checked="" type="checkbox"/> Chemical/Biological Contamination | <input checked="" type="checkbox"/> Data Integrity Loss | <input checked="" type="checkbox"/> Identity Theft |
| <input checked="" type="checkbox"/> Blackmail | <input checked="" type="checkbox"/> Denial of Service Attacks | <input checked="" type="checkbox"/> Malicious Code |
| <input checked="" type="checkbox"/> Bomb Threats | <input checked="" type="checkbox"/> Earthquakes | <input type="checkbox"/> Power Loss |
| <input type="checkbox"/> Burglary/Break In/Robbery | <input type="checkbox"/> Eavesdropping/Interception | <input checked="" type="checkbox"/> Sabotage/Terrorism |
| <input type="checkbox"/> Cold/Frost/Snow | <input checked="" type="checkbox"/> Errors (Configuration and Data Entry) | <input checked="" type="checkbox"/> Storms/Hurricanes |
| <input checked="" type="checkbox"/> Communications Loss | <input checked="" type="checkbox"/> Fire (False Alarm, Major, and Minor) | <input type="checkbox"/> Substance Abuse |
| <input checked="" type="checkbox"/> Computer Intrusion | <input checked="" type="checkbox"/> Flooding/Water Damage | <input checked="" type="checkbox"/> Theft of Assets |
| <input type="checkbox"/> Computer Misuse | <input type="checkbox"/> Fraud/Embezzlement | <input checked="" type="checkbox"/> Theft of Data |
| <input checked="" type="checkbox"/> Data Destruction | | <input type="checkbox"/> Vandalism/Rioting |

Answer: (Other Risks) Insider Threat (professional Criminals, disgruntled personnel, foreign agents, terrorists, physical security), External Threat (external hacker, worms & viruses, Trojans, malware), Environmental Threat (Tornadoes, Man Made threats).

Explain what security controls are being used to mitigate these risks. (Check all that apply)

- | | | |
|--|---|---|
| <input checked="" type="checkbox"/> Access Control | <input checked="" type="checkbox"/> Contingency Planning | <input checked="" type="checkbox"/> Personnel Security |
| <input checked="" type="checkbox"/> Audit and Accountability | <input checked="" type="checkbox"/> Identification and Authentication | <input checked="" type="checkbox"/> Physical and Environmental Protection |
| <input checked="" type="checkbox"/> Awareness and Training | <input checked="" type="checkbox"/> Incident Response | <input checked="" type="checkbox"/> Risk Management |
| <input checked="" type="checkbox"/> Certification and Accreditation Security Assessments | | |
| <input checked="" type="checkbox"/> Configuration Management | <input checked="" type="checkbox"/> Media Protection | |

Answer: (Other Controls)

PIA: PIA Assessment

Identify what choices were made regarding the project/system or collection of information as a result of performing the PIA.

Answer: Restricted access and security was part of the original design to maintain the integrity of financial data and vendor data. The system is 100% contained behind the firewall of the VA's Austin Information Technology Center. State of the art data security audits and safeguards are used to protect the systems that operate at this facility. Data can only be accessed by VA employees. The personnel accessing the data must complete all of the VA's required background checks and receive specific permission from their servicing Information Security Officer (ISO) before being granted the accesses required to view Privacy Information contained within DFAS.

Availability Assessment: If the data being collected is not available to process for any reason what will the potential impact be upon the system or organization?
(Choose One)

- ☒ The potential impact is **high** if the loss of availability could be expected to have a severe or catastrophic adverse effect on operations, assets or individuals.
- ☐ The potential impact is **moderate** if the loss of availability could be expected to have a serious adverse effect on operations, assets or individuals.
- ☐ The potential impact is **low** if the loss of availability could be expected to have a limited adverse effect on operations, assets or individuals.

Integrity Assessment: If the data being collected has been corrupted for any reason what will the potential impact be upon the system or organization?
(Choose One)

- ☒ The potential impact is **high** if the loss of integrity could be expected to have a severe or catastrophic adverse effect on operations, assets or individuals.
- ☐ The potential impact is **moderate** if the loss of integrity could be expected to have a serious adverse effect on operations, assets or individuals.
- ☐ The potential impact is **low** if the loss of integrity could be expected to have a limited adverse effect on operations, assets or individuals.

Confidentiality Assessment: If the data being collected has been shared with unauthorized individuals what will the potential impact be upon the system or organization? (Choose One)

- ☒ The potential impact is **high** if the loss of confidentiality could be expected to have a severe or catastrophic adverse effect on operations, assets or individuals.
- ☐ The potential impact is **moderate** if the loss of confidentiality could be expected to have a serious adverse effect on operations, assets or individuals.
- ☐ The potential impact is **low** if the loss of confidentiality could be expected to have a limited adverse effect on operations, assets or individuals.

The controls are being considered for the project based on the selections from the previous assessments?

The minimum security requirements for our high impact system cover seventeen security-related areas with regard to protecting the confidentiality, integrity, and availability of VA information systems and the information processed, stored, and transmitted by those systems. The security-related areas include: access control; awareness and training; audit and accountability; certification, accreditation, and security assessments; configuration management; contingency planning; identification and authentication; incident response; maintenance; media protection; physical and environmental protection; planning; personnel security; risk assessment; systems and services acquisition; system and communications protection; and system and information integrity. Our facility employs all security controls in the respective high impact security control baseline unless specific exceptions have been allowed based on the tailoring guidance provided in NIST Special Publication 800-53 and specific VA directives.

Please add additional controls:

(FY 2011) PIA: Additional Comments

Add any additional comments or information that may have been left out for any question. Please indicate the question you are responding to and then add your comments.

(FY 2011) PIA: VBA Minor Applications

Which of these are sub-components of your system?

Access Manager	Automated Sales Reporting (ASR)	Automated Folder Processing System (AFPS)
Actuarial	BCMA Contingency Machines	Automated Medical Information Exchange II (AIME II)
Appraisal System	Benefits Delivery Network (BDN)	Automated Medical Information System (AMIS)290
ASSISTS	Centralized Property Tracking System	Automated Standardized Performance Elements Nationwide (ASPEN)
Awards	Common Security User Manager (CSUM)	Centralized Accounts Receivable System (CARS)
Awards	Compensation and Pension (C&P)	Committee on Waivers and Compromises (COWC)
Baker System	Control of Veterans Records (COVERS)	Compensation and Pension (C&P) Record Interchange (CAPRI)
Bbraun (CP Hemo)	Control of Veterans Records (COVERS)	Compensation & Pension Training Website
BDN Payment History	Control of Veterans Records (COVERS)	Corporate Waco, Indianapolis, Newark, Roanoke, Seattle (Corporate WINRS)
BIRLS	Courseware Delivery System (CDS)	Distribution of Operational Resources (DOOR)
C&P Payment System	Dental Records Manager	Educational Assistance for Members of the Selected Reserve Program CH 1606
C&P Training Website	Education Training Website	Electronic Performance Support System (EPSS)
CONDO PUD Builder	Electronic Appraisal System	Enterprise Wireless Messaging System (Blackberry)
Corporate Database	Electronic Card System (ECS)	Financial Management Information System (FMI)
Data Warehouse	Electronic Payroll Deduction (EPD)	Hearing Officer Letters and Reports System (HOLAR)
EndoSoft	Eligibility Verification Report (EVR)	Inquiry Routing Information System (IRIS)
FOCAS	Fiduciary Beneficiary System (FBS)	Modern Awards Process Development (MAP-D)
Inforce	Fiduciary STAR Case Review	Personnel and Accounting Integrated Data and Fee Basis (PAID)
INS - BIRLS	Financial and Accounting System (FAS)	Personal Computer Generated Letters (PCGL)
Insurance Online	Insurance Unclaimed Liabilities	Personnel Information Exchange System (PIES)
Insurance Self Service	Inventory Management System (IMS)	Personnel Information Exchange System (PIES)
LGY Home Loans	LGY Centralized Fax System	Post Vietnam Era educational Program (VEAP) CH 32
LGY Processing	Loan Service and Claims	Purchase Order Management System (POMS)
Mobilization	Loan Guaranty Training Website	Reinstatement Entitlement Program for Survivors (REAPS)
Montgomery GI Bill	Master Veterans Record (MVR)	Reserve Educational Assistance Program CH 1607
MUSE	Mental Health Assistant	Service Member Records Tracking System
Omnicell	National Silent Monitoring (NSM)	Survivors and Dependents Education Assistance CH 35
Priv Plus	Powerscribe Dictation System	Systematic Technical Accuracy Review (STAR)
RAI/MDS	Rating Board Automation 2000 (RBA2000)	Training and Performance Support System (TPSS)
Right Now Web	Rating Board Automation 2000 (RBA2000)	VA Online Certification of Enrollment (VA-ONCE)
SAHSHA	Rating Board Automation 2000 (RBA2000)	VA Reserve Educational Assistance Program
Script Pro	Records Locator System	Veterans Appeals Control and Locator System (VACOLS)
SHARE	Review of Quality (ROQ)	Veterans Assistance Discharge System (VADS)
SHARE	Search Participant Profile (SPP)	Veterans Exam Request Info System (VERIS)
SHARE	Spinal Bifida Program Ch 18	Veterans Service Representative (VSR) Advisor
Sidexis	State Benefits Reference System	Vocational Rehabilitation & Employment (VR&E) CH 31
Synquest	State of Case/Supplemental (SOC/SSOC)	Waco Indianapolis, Newark, Roanoke, Seattle (WINRS)

VBA Data Warehouse
VBA Training Academy
Veterans Canteen Web
VIC
VR&E Training Website
Web LGY

Telecare Record Manager
VBA Enterprise Messaging System
Veterans On-Line Applications (VONAPP)
Veterans Service Network (VETSNET)
Web Electronic Lender Identification

Web Automated Folder Processing System (WAFPS)
Web Automated Reference Material System (WARMS)
Web Automated Verification of Enrollment
Web-Enabled Approval Management System (WEAMS)
Web Service Medical Records (WebSMR)
Work Study Management System (WSMS)

Explain any minor application that are associated with your installation that does not appear in the list above. Please provide name, brief description, and any comments you may wish to include.

Name
Description
Comments
Is PII collected by this min or application?
Does this minor application store PII?
If yes, where?
Who has access to this data?

Name
Description
Comments
Is PII collected by this min or application?
Does this minor application store PII?
If yes, where?
Who has access to this data?

Name
Description
Comments
Is PII collected by this min or application?
Does this minor application store PII?
If yes, where?
Who has access to this data?

(FY 2011) PIA: VISTA Minor Applications

Which of these are sub-components of your system?

ASISTS	Beneficiary Travel	Accounts Receivable	Adverse Reaction Tracking
Bed Control	Care Management	ADP Planning (PlanMan)	Authorization/ Subscription
CAPRI	Care Tracker	Bad Code Med Admin	Auto Replenishment/ Ward Stock
CMOP	Clinical Reminders	Clinical Case Registries	Automated Info Collection Sys
Dental	CPT/ HCPCS Codes	Clinical Procedures	Automated Lab Instruments
Dietetics	DRG Grouper	Consult/ Request Tracking	Automated Med Info Exchange
Fee Basis	DSS Extracts	Controlled Substances	Capacity Management - RUM
GRECC	Education Tracking	Credentials Tracking	Capacity Management Tools
HINQ	Engineering	Discharge Summary	Clinical Info Resource Network
IFCAP	Event Capture	Drug Accountability	Clinical Monitoring System
Imaging	Extensible Editor	EEO Complaint Tracking	Enrollment Application System
Kernal	Health Summary	Electronic Signature	Equipment/ Turn-in Request
Kids	Incident Reporting	Event Driven Reporting	Gen. Med.Rec. - Generator
Lab Service	Intake/ Output	External Peer Review	Health Data and Informatics
Letterman	Integrated Billing	Functional Independence	ICR - Immunology Case Registry
Library	Lexicon Utility	Gen. Med. Rec. - I/O	Income Verification Match
Mailman	List Manager	Gen. Med. Rec. - Vitals	Incomplete Records Tracking
Medicine	Mental Health	Generic Code Sheet	Interim Mangement Support
MICOM	MyHealthEVet	Health Level Seven	Master Patient Index Vista
NDBI	National Drug File	Hospital Based Home Care	Missing Patient Reg (Original) A4EL
NOIS	Nursing Service	Inpatient Medications	Order Entry/ Results Reporting
Oncology	Occurrence Screen	Integrated Patient Funds	PCE Patient Care Encounter
PAID	Patch Module	MCCR National Database	Pharmacy Benefits Mangement
Prosthetics	Patient Feedback	Minimal Patient Dataset	Pharmacy Data Management
QUASER	Police & Security	National Laboratory Test	Pharmacy National Database
RPC Broker	Problem List	Network Health Exchange	Pharmacy Prescription Practice
SAGG	Progress Notes	Outpatient Pharmacy	Quality Assurance Integration
Scheduling	Record Tracking	Patient Data Exchange	Quality Improvement Checklist
Social Work	Registration	Patient Representative	Radiology/ Nuclear Medicine
Surgery	Run Time Library	PCE Patient/ HIS Subset	Release of Information - DSSI
Toolkit	Survey Generator	Security Suite Utility Pack	Remote Order/ Entry System
Unwinder	Utilization Review	Shift Change Handoff Tool	Utility Management Rollup
VA Fileman	Visit Tracking	Spinal Cord Dysfunction	CA Verified Components - DSSI
VBECS	VistALink Security	Text Integration Utilities	Vendor - Document Storage Sys
VDEF	Women's Health	VHS & RA Tracking System	Visual Impairment Service Team ANRV
VistALink		Voluntary Timekeeping	Voluntary Timekeeping National

Explain any minor application that are associated with your installation that does not appear in the list above. Please provide name, brief description, and any comments you may wish to include.

Name

Description

Comments

Is PII collected by this minor application?

Does this minor application store PII?

If yes, where?

Who has access to this data?

Name

Description

Comments

Is PII collected by this minor application?

Does this minor application store PII?

If yes, where?

Who has access to this data?

Name

Description

Comments

Is PII collected by this minor application?

Does this minor application store PII?

If yes, where?

Who has access to this data?

(FY 2011) PIA: Minor Applications

Which of these are sub-components of your system?

1184 Web	Agent Cashier	Administrative Data Repository (ADR)
A4P	Air Fortress	Automated Access Request
ADT	Auto Instrument	Bed Board Management System
BDN 301	Cardiff Teleform	Cardiology Systems (stand alone servers from the network)
CP&E	CHECKPOINT	Clinical Data Repository/Health Data Repository
DRM Plus	Data Innovations	Combat Veteran Outreach
DSIT	DELIVEREX	Committee on Waiver and Compromises
ENDSOFT	DSS Quadramed	Crystal Reports Enterprise
EYECAP	EKG System	DICTATION-Power Scribe
Genesys	ePROMISE	EDS Whiteboard (AVJED)
ICB	Lynx Duress Alarm	Embedded Fragment Registry
KOWA	Mumps AudioFAX	Enterprise Terminology Server & VHA Enterprise Terminology Services
MHTP	Onvicord (VLOG)	Financial and Accounting System (FAS)
NOAHLINK	P2000 ROBOT	Financial Management System (FMS)
Omniceil	PACS database	Health Summary Contingency
Optifill	PIV Systems	Microsoft Active Directory
PICIS OR	Remedy Application	Microsoft Exchange E-mail System
Q-Matic	Traumatic Brain Injury	Military/Vet Eye Injury Registry
RAFT	VAMedSafe	Personal Computer Generated Letters
RALS	VBA Data Warehouse	QMSI Prescription Processing
SAN	VHAHUNAPP1	Scanning Exam and Evaluation System
Sentillion	VHAHUNFPC1	Tracking Continuing Education
Stellant	VISTA RAD	VA Conference Room Registration
Stentor	Whiteboard	

Explain any minor application that are associated with your installation that does not appear in the list above. Please

Name
Description
Comments
Is PII collected by this minor application?
Does this minor application store PII?
If yes, where?
Who has access to this data?

Name
Description
Comments
Is PII collected by this minor application?
Does this minor application store PII?
If yes, where?
Who has access to this data?

Name
Description
Comments
Is PII collected by this minor application?
Does this minor application store PII?
If yes, where?
Who has access to this data?

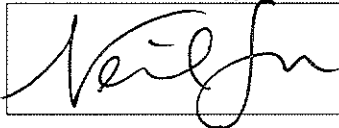
(FY 2011) PIA: Final Signatures

Facility Name: CDCO > AITC > VA > Defense Finance Accountability Service (DFAS) Secure ePayroll Transmission

Title:	Name:	Phone:	Email:
Privacy Officer:	Amy Howe	512-326-6217	amy.howe1@va.gov

Digital Signature Block

Information Security Officer:	Neil Cruz	(202) 461-6254	neil.cruz@va.gov
-------------------------------	-----------	----------------	------------------



Digital Signature Block

System Owner/ Chief Information Officer:	John Rucker	512-326-6422	John.Rucker@va.gov
--	-------------	--------------	--------------------

Digital Signature Block

Data Owner:	Roy Coles	202-461-6105	roy.coles@va.gov
-------------	-----------	--------------	------------------

Digital Signature Block

Other Titles:	0	0	0
---------------	---	---	---

Digital Signature Block

Date of Report:	02/2011
OMB Unique Project Identifier	029-00-01-19-01-1330-00
Project Name	CDCO > AITC > VA > Defense Finance Accountability Service (DFAS) Secure ePayroll Transmission

(FY 2011) PIA: Final Signatures

Facility Name:

AITC

Title:	Name:	Phone:	Email:
--------	-------	--------	--------

Privacy Officer:

Amy Howe

512-326-6217

Amy.Howe1@va.gov

**Amy J.
Howe**

Digital Signature Block

Digitally signed by: Amy J. Howe
DN: CN = Amy J. Howe C = US O = U.S.
Government OU = Department of Veterans Affairs
Date: 2011.03.24 10:54:21 -06'00'

Information Security Officer:

Digital Signature Block

System Owner/ Chief Information Officer:

John Rucker

512-326-6422

John.Rucker@va.gov



Digital Signature Block

Information Owner:

Digital Signature Block

Other Titles:

Digital Signature Block

Date of Report:

OMB Unique Project Identifier

Project Name

(FY 2011) PIA: Final Signatures

Facility Name: CDCO > AITC > VA > Defense Finance Accountability Service (DFAS) Secure ePayroll Transmission

Title:	Name:	Phone:	Email:
Privacy Officer:	Amy Howe	512-326-6217	amy.howe1@va.gov

Digital Signature Block

Information Security Officer:	Neil Cruz	(202) 461-6254	neil.cruz@va.gov
-------------------------------	-----------	----------------	------------------

Digital Signature Block

System Owner/ Chief Information Officer:	John Rucker	512-326-6422	John.Rucker@va.gov
--	-------------	--------------	--------------------

Digital Signature Block

Data Owner:	Roy Coles	202-461-6105	roy.coles@va.gov
-------------	-----------	--------------	------------------

Digital Signature Block

Other Titles:	0	0	0
---------------	---	---	---

Digital Signature Block

Date of Report: 02/2011

OMB Unique Project Identifier 029-00-01-19-01-1330-00

CDCO > AITC > VA > Defense
Finance Accountability Service

Project Name (DFAS) Secure ePayroll
Transmission